Imaging Device Guidelines for Syracuse University

Syracuse University – Information Technology and Services

Information Security Guideline – G0101

1.0 Scope

This document aims to create a guideline for securing all printing, scanning and faxing devices owned by Syracuse University (SU) and connected to the SU network.

2.0 Purpose

The purpose of this document is to provide a consistent, secure configuration approach for all imaging devices that fall in scope of this guideline including networked printers, multi---function devices, scanners, copiers and faxes, as well as protect information generated and assure the accuracy and security of that information for all SU departments.

3.0 Guideline

Any network attached imaging device should be "hardened" or protected from network attack. There are many different manufacturers and models of imaging devices hence no one set of instructions can be written to cover all. This document aims to provide an overall guideline of the most common hardening techniques.

3.1 **Change default passwords**. Most devices can be administered via the network by use of a default username and password, this password should be changed to strong administrator passwords. Access to this password should be limited to only those staff members that need it for managing the device.

3.2 **Change default SNMP strings**. Many devices run SNMP with default community strings of "public" and "private". The SNMP Get (read only) community string should be changed to the SU Default printer string of "susnmp". SNMP Set (read-write) should only be enabled on an as needed basis, and the community string should follow the same complexity conventions and access as the administrative password.

3.3 **Upgrade software/firmware to latest version**. Most devices support upgrades to firmware and software installed by the manufacturer. Admins should check to make sure the code is at its highest version, and if not, download and install it. Administrators should keep informed of software releases and upgrade as consistent with change control process.

3.4 **Assign an internal IP address**. If the device does not need to communicate with the internet, it should be placed on the internal, RFC 1918 IP address space (commonly known as the "10---Net" at SU since these addresses are in the form of 10.230.x.x).

3.5 **Turn off unneeded services**. Many devices support Telnet, FTP, and Web Access among others. If possible, turn off any of these services that will not be used.

3.6 **Turn off unneeded printing protocols.** Limit the print, copy, scan and/or fax services to the required protocols (disable other services like AppleTalk, Netware etc.).

3.7 **Limit network access to device.** If it makes sense (based on the intended use of the device), limit access to the device via local access control lists or firewalls. Remote access can be enabled through SU VPN solution.

3.8 **Logging.** Enable logging if required only. Ensure that logs are retained accordingly to the Data Retention Policy at SU.

3.9 **Limit storage of data**. Many devices are now storing files or images of documents on a local, internal hard drive or other storage device. Administrators should become familiar with how this data is stored and enable any security mechanisms (like automatic deletion/overwrite of temporary data and or hard---drive encryption) as supported by device to limit or protect the data that gets stored. Users should NOT store any SU confidential data on the device. At times of maintenance, request the vendor's technician to refresh and format the hard-drive.

3.10 **Physically secure the device.** Depending on the use of the device, administrators should consider device's physical location and who potentially has access. The device should be as physically secure as is practical for its intended use.

If any violations are known, they should be reported to Syracuse University's Information Security Office at itsecurity@listserv.syr.edu

4.0 Referred Documents, Web Pages and Contact Information

Item	**Location/Info**
Standard: *Syracuse University Information Security Standard*	http://its.syr.edu/security/standards/ITSecurity---standard.pdf
Syracuse University Record Retention Policy	http://rm.syr.edu/ret---adm.html
Contact: Director of Information Security	Christopher Croad ccroad@syr.edu

Document Info

Version:	2.0
Effective Date:	Jan 25, 2015
Date of Last Review	March 27, 2015
Date of Next Mandatory Review	June 24, 2016